Esther Omlin: Jeder sollte sich vor Datendiebstahl schützen

Esther Omlin: Phishing-Angriffe sind strafrechtlich nur schwer zu verfolgen

Das illegale Abgreifen persönlicher Passwörter und Daten ist im Internet inzwischen ein alltäglicher Vorgang. Esther Omlin erklärt, warum es so schwierig ist, eine strafrechtliche Handhabe gegen Phishing zu finden und wie man sich gegen derartige Angriffe schützen sollte.

Wie jeder Internet-Nutzer weiss auch Dr. Iur. Esther Omlin, dass auf Webseiten immer wieder persönliche Daten und Passwörter angegeben werden müssen. Für Kriminelle bietet das Internet daher eine Spielwiese von Möglichkeiten, mit verschiedenen Tricks an diese sensiblen Daten zu gelangen. Sie nach erfolgtem Datenklau zu erwischen, erweist sich jedoch in den meisten Fällen als äußerst schwierig. Warum das so ist, wie die Rechtslage bei Phishing aussieht und was jeder selbst tun kann, um sich vor dem Diebstahl persönlicher Daten zu schützen, beschreibt Esther Omlin:

- Wie Phishing-Angriffe ablaufen
- Wie die Rechtslage zu Phishing aussieht
- Was Polizei und Justiz bei Diebstahl persönlicher Daten tun können
- Wie man vermeiden kann, ein Phishing-Opfer zu werden

WIE PHISHING-ANGRIFFE ABLAUFEN

Kriminelle gehen beim Stehlen von Daten immer wieder äusserst kreativ vor, doch gibt es typische Merkmale, die jeder Phishing-Angriff aufweist, erklärt Esther Omlin:

- Man wird aufgefordert, aus einem bestimmten Grund seine Daten anzugeben, meist per E-Mail, die einen Link zu einer gefälschten Webseite beinhaltet. Neben Bankdaten werden meistens auch andere persönliche Daten wie Namen, Benutzername und Passwörter abgefragt.
- Phishing-Mails täuschen durch Gestaltung, Absender und Inhalt vor, dass es sich um bekannte Institute oder Firmen handelt und die Wahrscheinlichkeit hoch ist, dass der Adressat dort ein Benutzerkonto führt.
- Möglich ist auch, dass die Webauftritte seriöser Unternehmen gehackt und Phishing-Seiten eingebaut werden – eine vor allem beim E-Banking bekannte Problematik.

WIE DIE RECHTSLAGE ZU PHISHING AUSSIEHT

Esther Omlin weist darauf hin, dass es im Schweizerischen Strafgesetzbuch StGB derzeit noch keinen eigenen Straftatbestand zu Phishing gibt. Oft können jedoch andere Artikel angewendet werden, etwa unbefugte Datenbeschaffung, unbefugtes Eindringen in ein Datenverarbeitungssystem, Sachbeschädigung, betrügerischer Missbrauch einer Datenverarbeitungsanlage, Urkundenfälschung oder Geldwäscherei.

WAS POLIZEI UND JUSTIZ BEI DIEBSTAHL PERSÖNLICHER DATEN TUN KÖNNEN

Esther Omlin beschreibt das Problem: Phishing ist enorm schwer nachzuverfolgen, was daran liegt, dass die Täter zumeist im Ausland ansässige Dienste zur Erstellung und zum Hosting von Phishing-Seiten nutzen. Des Weiteren werden die gestohlenen Daten in den meisten Fällen weiterverkauft und dann wieder von anderen Kriminellen verwendet. Für Polizei und Justiz bietet sich hier kaum eine Handhabe und Fahndungserfolge sind eher selten. Umso wichtiger ist es daher, dass jeder sich selbst vor solcherart Angriffen schützt, betont Esther Omlin.

WIE MAN VERMEIDEN KANN, EIN PHISHING-OPFER ZU WERDEN

Grundsätzliches Misstrauen ist angebracht, wenn E-Mails im Postfach auftauchen, in denen direkt oder über einen Link die Eingabe persönlicher Daten verlangt wird. Auch wenn Konsequenzen wie Geldverlust, Strafanzeige oder Kartensperrung angedroht werden – als Empfänger gilt es, stets im Hinterkopf zu behalten, dass seriöse Dienstanbieter wie Banken, die Post, Online-Auktionsanbieter, Behörden und selbst Shopping-Portale niemals in E-Mails oder am Telefon zur Angabe von Passwörtern, Bankverbindungen oder Kreditkartendaten auffordern. Solche E-Mails sollten konsequent sofort gelöscht werden, ohne auf Links zu klicken oder zu antworten, rät Esther Omlin.